




**LAC
DMH**
LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT INFORMATION TECHNOLOGY AND SECURITY	POLICY NO. 555.02	EFFECTIVE DATE 04/20/2005	PAGE 1 of 9
APPROVED BY:  Director	SUPERSEDES 500.42 04/20/2005	ORIGINAL ISSUE DATE 04/20/2005	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To provide direction for the development and implementation of data security policies and procedures, and to identify the data security officials and their responsibilities.

POLICY

- 2.1 The Los Angeles County Department of Mental Health (LACDMH) is responsible for securing all electronic data, including Protected Health Information (PHI) and other confidential information, while complying with the security requirements of all applicable regulatory, compliance, and accreditation sources, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Medicare, and Medi-Cal.
- 2.2 LACDMH must develop data security policies and procedures to ensure the security of PHI and other confidential information, and the hardware and systems used to obtain, utilize, and maintain such information.
- 2.3 All LACDMH Workforce Members must comply with provisions of the LACDMH data security policies. Any Workforce Member who fails to comply will be subject to disciplinary action in accordance with LACDMH Policy No. 605.01, Discipline; Disciplinary Action; Civil Service Rule 18.031; and the LACDMH Employee Reference Manual.
- 2.4 To ensure compliance with the provisions of this policy, the following responsibilities have been designated to the following data security officials:
 - 2.4.1 LACDMH Departmental Information Security Officer (DISO)



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY AND SECURITY	555.02	04/20/2005	2 of 9

- 2.4.1.1 LACDMH must designate a DISO that is responsible for the development, implementation, and maintenance of LACDMH data security policies, procedures, and guidelines.
- 2.4.1.2 The LACDMH DISO will assist LACDMH managers in the risk analysis and management process.
- 2.4.1.3 The duties of the LACDMH DISO include, but are not limited, to the following:
1. Provide information security related technical, regulatory, and policy leadership;
 2. Facilitate the development and implementation of the LACDMH information security policies and procedures;
 3. Coordinate information security efforts across the facilities within LACDMH in alignment with Countywide security policies;
 4. Direct continuing information security training and education efforts;
 5. Represent LACDMH at the County Information Security Steering Committee (ISSC);
 6. Report to the LACDMH Chief Information Officer;
 7. Ensure LACDMH is in compliance with all laws, rules, and regulations as they relate to the proper handling of data and electronic media;
 8. Recommend new security standards as technology changes;
 9. Coordinate LACDMH-wide security software and hardware purchasing and licensing; and
 10. Review and approve data security implementation and risk management efforts.
- 2.4.1.4 The LACDMH DISO or his/her designee must review and approve the Risk Analysis Report.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY AND SECURITY	555.02	04/20/2005	3 of 9

- 2.4.1.5 The LACDMH DISO or his/her designee must review and approve the LACDMH Facility Master Security Management Report, LACDMH Policy No. 550.01, Security Management Process: LACDMH Risk Management.
- 2.4.1.6 The LACDMH DISO or his/her designee must assist System Managers/Owners in implementing access authorization procedures and determining the appropriate technical access controls.
- 2.4.1.7 The LACDMH DISO or his/her designee will coordinate the Departmental Computer Emergency Response Team (DCERT).
- 2.4.1.8 The LACDMH DISO or his/her designee and DCERT are responsible for determining the appropriate level of response to a security incident.
- 2.4.1.9 The LACDMH DISO or his/her designee must represent the Department at the County Computer Emergency Response Team (CCERT) as the primary DCERT member.
- 2.4.1.10 Creating and periodically updating the Facility Master Security Management Report.
- 2.4.1.11 Working with System Managers/Owners, LACDMH managers and supervisors, and the LACDMH Human Resources Bureau to develop workforce security procedures and to coordinate those activities necessary to implement the workforce security procedures.

2.4.2 LACDMH Chief Information Officer (CIO)

The duties of the LACDMH CIO or his/her designee include, but are not limited to, the following:



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY AND SECURITY	555.02	04/20/2005	4 of 9

- 2.4.2.1 Management responsibility over all systems within the Department.
- 2.4.2.2 Ensuring that System Managers/Owners conduct risk assessments for their data resources and information systems in accordance with LACDMH procedures.
- 2.4.2.3 Ensuring that System Managers/Owners develop plans to implement the Facility Master Security Management Report's recommended safeguards and actions.
- 2.4.2.4 Ensuring that System Managers/Owners establish, document, and implement procedures for reviewing information systems activity, including but not limited to audit logs, problem logs, system access reports, change control logs, and security incident reports.
- 2.4.2.5 Ensuring that System Managers/Owners authorize access to information resources under their control on a "need to know basis" for carrying out the essential job functions of the workforce members.
- 2.4.2.6 Ensuring that System Managers/Owners implement procedures for establishing LACDMH Workforce Member access to electronic information for example, through access to a workstation, transaction, program, process, or other mechanism that is both necessary and appropriate for the job functions of the Workforce Member.
- 2.4.2.7 Ensuring that System Managers/Owners implement procedures that modify a user's right of access to a workstation, transaction, program, process, or other mechanism, when such modification is necessary to align the Workforce Members' access with the Workforce Members' essential job functions.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY AND SECURITY	555.02	04/20/2005	5 of 9

2.4.2.8 Ensuring that the System Managers/Owners respond to security incidents and emergency situations in a manner authorized and directed by the DISO or his/her designee and DCERT.

2.4.3 System Managers/Owners

The System Managers/Owners security responsibilities include, but are not limited to the following:

2.4.3.1 Establishing rules for system use and protection of PHI and other confidential information as required by the LACDMH Policy No. 553.02, LACDMH Privacy and Security Compliance Program policy.

2.4.3.2 Working with LACDMH DISO to implement the LACDMH Policy No. 550.01, Security Management Process: LACDMH Risk Management.

2.4.3.3 Establishing, documenting, and implementing procedures for reviewing information systems activity, including but not limited to, audit logs, problem logs, system access reports, change control logs, and security incident reports.

2.4.3.4 Working with LACDMH DISO or his/her designee, LACDMH managers and supervisors, and LACDMH Human Resources to develop workforce security procedures and to coordinate those activities necessary to implement the workforce security procedures.

2.4.3.5 Implementing procedures for establishing LACDMH Workforce Member access to electronic information; for example, through access to a workstation, transaction, program, process, or other mechanism that is both necessary and appropriate for the job functions of the Workforce Member.



LACDMH
LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY AND SECURITY	555.02	04/20/2005	6 of 9

2.4.3.6 Ensuring that each Workforce Member with access has signed an acknowledgment of the LACDMH Policy No. 556.01, LACDMH Acceptable Use for County Information Technology Resources that (1) defines their responsibility for protecting the confidentiality, integrity, and availability of all DMH information resources and (2) identifies restrictions for utilizing those resources.

2.4.3.7 Determining the sensitivity and criticality of the resources for which they are responsible and developing, implementing, and maintaining the Contingency Plan that is commensurate with the criticality.

2.4.3.8 Ensuring that appropriate physical safeguards and technical security policies are implemented.

2.4.3.9 Defining the system's security requirements in its System Security Documentation.

2.4.3.10 Training and communicating to the Workforce Member the proper procedures for protecting the PHI and other confidential information.

2.4.4 LACDMH Human Resources Bureau (HRB)

The security responsibilities of the LACDMH HBR include, but are not limited to, the following:

2.4.4.1 Working with System Managers/Owners to ensure proper workforce clearance procedures are implemented.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY AND SECURITY	555.02	04/20/2005	7 of 9

2.4.4.2 Ensuring that each new workforce member receives and signs acknowledgment of LACDMH Policy No 556.01, Acceptable Use for County Information Technology Resources, during the new hire orientation and that each Workforce Member completes the acknowledgment during the annual Performance Evaluation process. Signed acknowledgments will be filed in the Workforce Member's official personnel folder.

2.4.4.3 Ensuring that all LACDMH personnel terminations, new hires, or internal transfers are communicated timely to the LACDMH DISO or his/her designee.

2.4.5 Workforce Managers and Supervisors

The security responsibilities of workforce managers and supervisors include, but are not limited to, the following:

2.4.5.1 Determining Workforce Members' access rights and levels based on the Workforce Members' job responsibilities and authorizing Workforce Members to have access to electronic data systems, the Internet, and Intranet systems.

2.4.5.2 Supervising the activities of LACDMH Workforce Members in relation to the use and Disclosure of electronic data.

2.4.5.3 Providing authorization and supervision to LACDMH Workforce Members and others who need to be in areas where confidential and/or sensitive information may be accessed, and observing appropriate safeguards to ensure those who may be exposed to confidential or sensitive information are made aware of the policies protecting that information.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY AND SECURITY	555.02	04/20/2005	8 of 9

2.4.5.4 Identifying and supervising LACDMH Workforce Members who work with confidential and/or sensitive information or who work in locations where confidential and/or sensitive information might be accessed.

2.4.5.5 Reporting any and all suspected and actual breaches of information security to the LACDMH DISO or Help Desk.

2.4.6 Workforce Member

The security responsibilities of all LACDMH Workforce Members include, but are not limited to, the following:

2.4.6.1 Complying with the provisions of all relevant data security policies and procedures. Including but not limited to the LACDMH Policy No. 553.02, LACDMH Privacy and Security Compliance Program; LACDMH Policy No. 556.01, LACDMH Acceptable Use for County Information Technology Resources; and LACDMH Policy No. 551.03, Workstation Use and Security.

2.4.6.2 Reporting any and all suspected and actual breaches of information security to the LACDMH DISO or Help Desk.

DEFINITIONS

Terms used in this policy and subsequent LACDMH data security policies and procedures are included in the LACDMH Information Security Glossary (Attachment 1).

AUTHORITY

1. **MANDATED BY** 45 Code of Federal Regulations (CFR) Part 164, §164.308(a)(2)
2. Health Insurance Portability and Accountability Act (HIPAA) of 1996 Public Law 104-91
3. Board of Supervisors Policy No. 6.100, Information Technology and Security Policy



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY AND SECURITY	555.02	04/20/2005	9 of 9

CROSS REFERENCE

Board of Supervisors Policy Nos.:

- 6.101 Use of County Information Technology Resources
- 6.102 Countywide Antivirus Security Policy
- 6.103 Countywide Computer Security Threat Responses
- 6.104 Electronic Communications
- 6.105 Internet Usage Policy
- 6.106 Physical Security
- 6.107 Information Technology Risk Assessment
- 6.108 Auditing and Compliance

ATTACHMENT (HYPERLINKED)

1. [LACDMH Information Security Glossary](#)

REVIEW DATE

This policy shall be reviewed on or before January 2010.